

Automatizace v boji pro moderním kybernetickým hrozbám

Jakub Jiříček, CISSP, CNSE

Systems Engineer, Eastern Europe

jjiricek@paloaltonetworks.com



WildFire Stats 2018

300M+

Never before seen samples every month demonstrates our unique data set

45%

Malware detected by WildFire is unknown in Virus Total

1- PE, PE64 (Windows)

2- Android APK ↑

3- DLL (Windows)

4- PDF (Adobe)

5- ELF (Linux) ↑

Top file type trends



unit 42



CYBER
THREAT
ALLIANCE

22,000+

WildFire Customers growing every month

40%

Zero-day malware detected by WildFire were not seen by the top six antivirus vendors at the time of detection

8%

Malware delivered over applications other than web and email
(FTP, SMB)

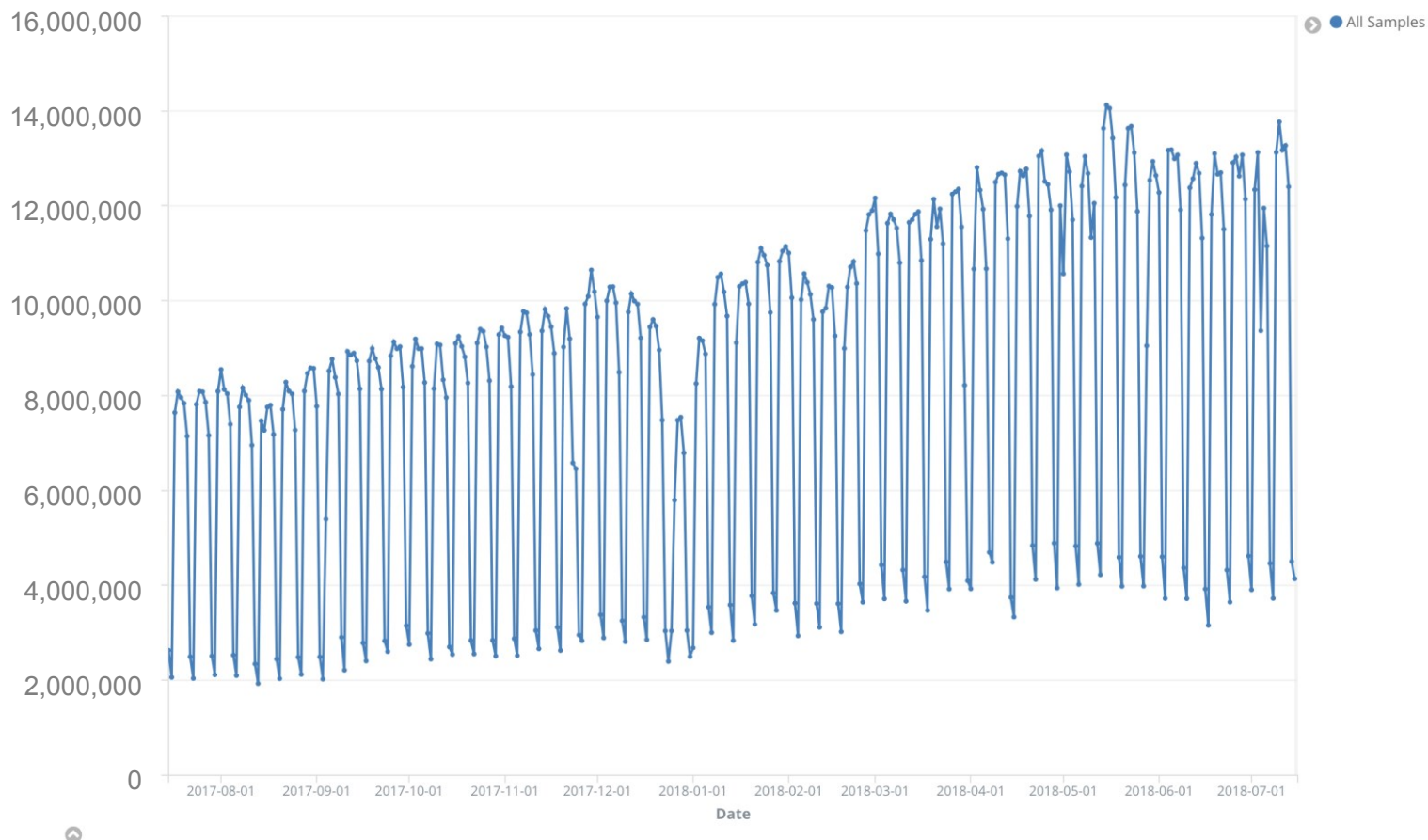
230K

- New high quality protections delivered daily to the platform within 5 minutes

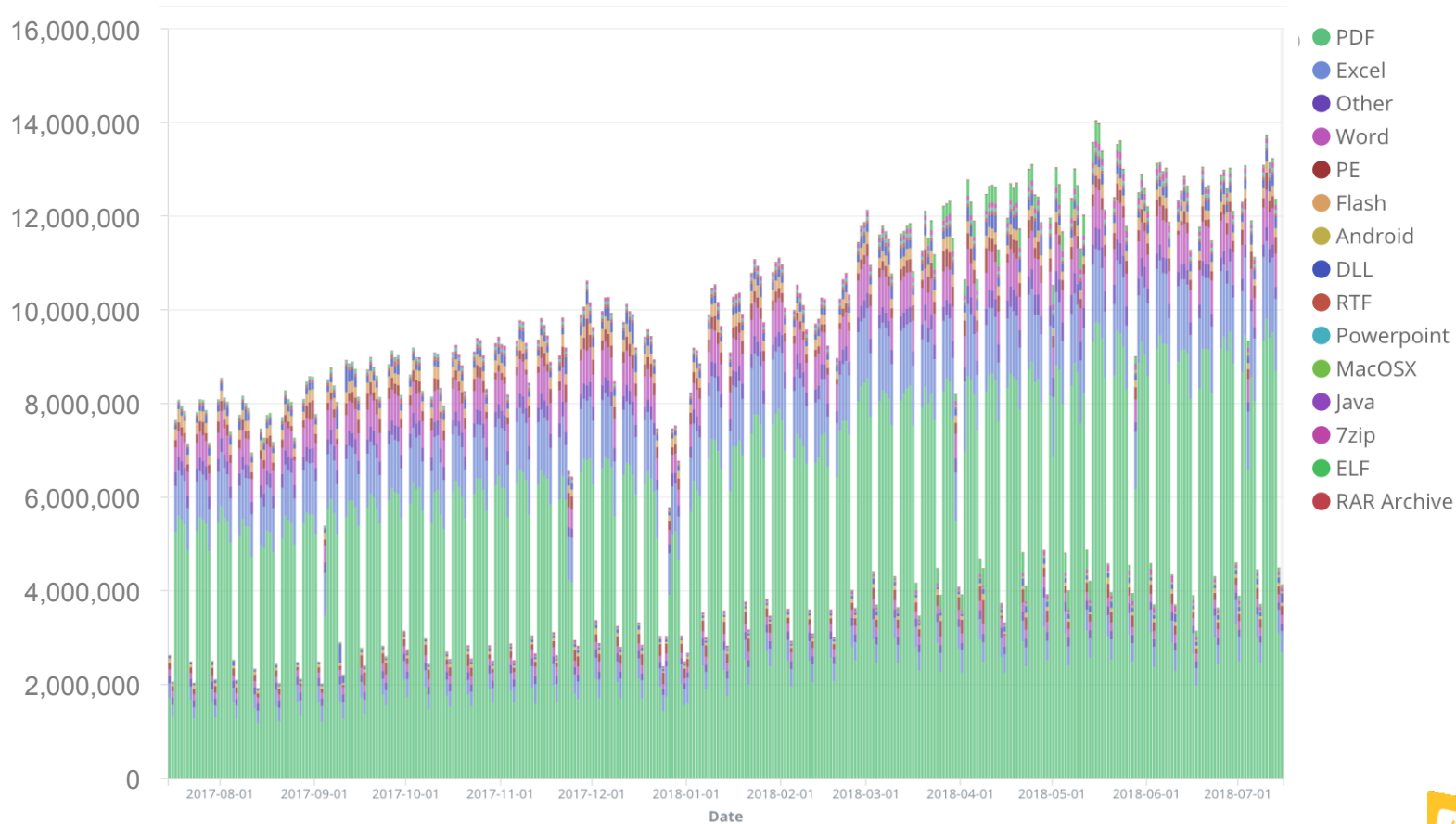
- IP, DNS, C2, URL, WF-AV



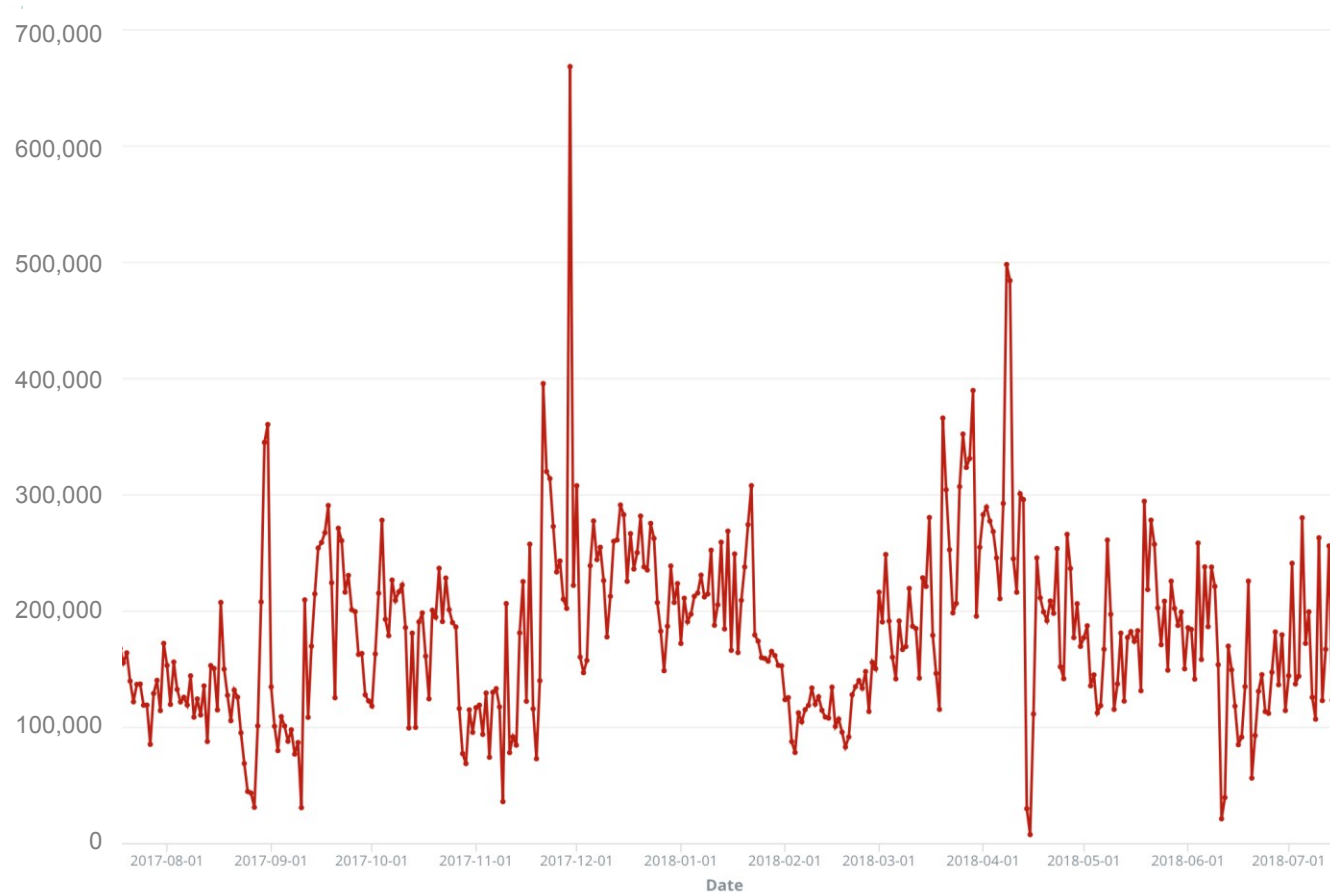
Denní vzorky: všechny výsledky



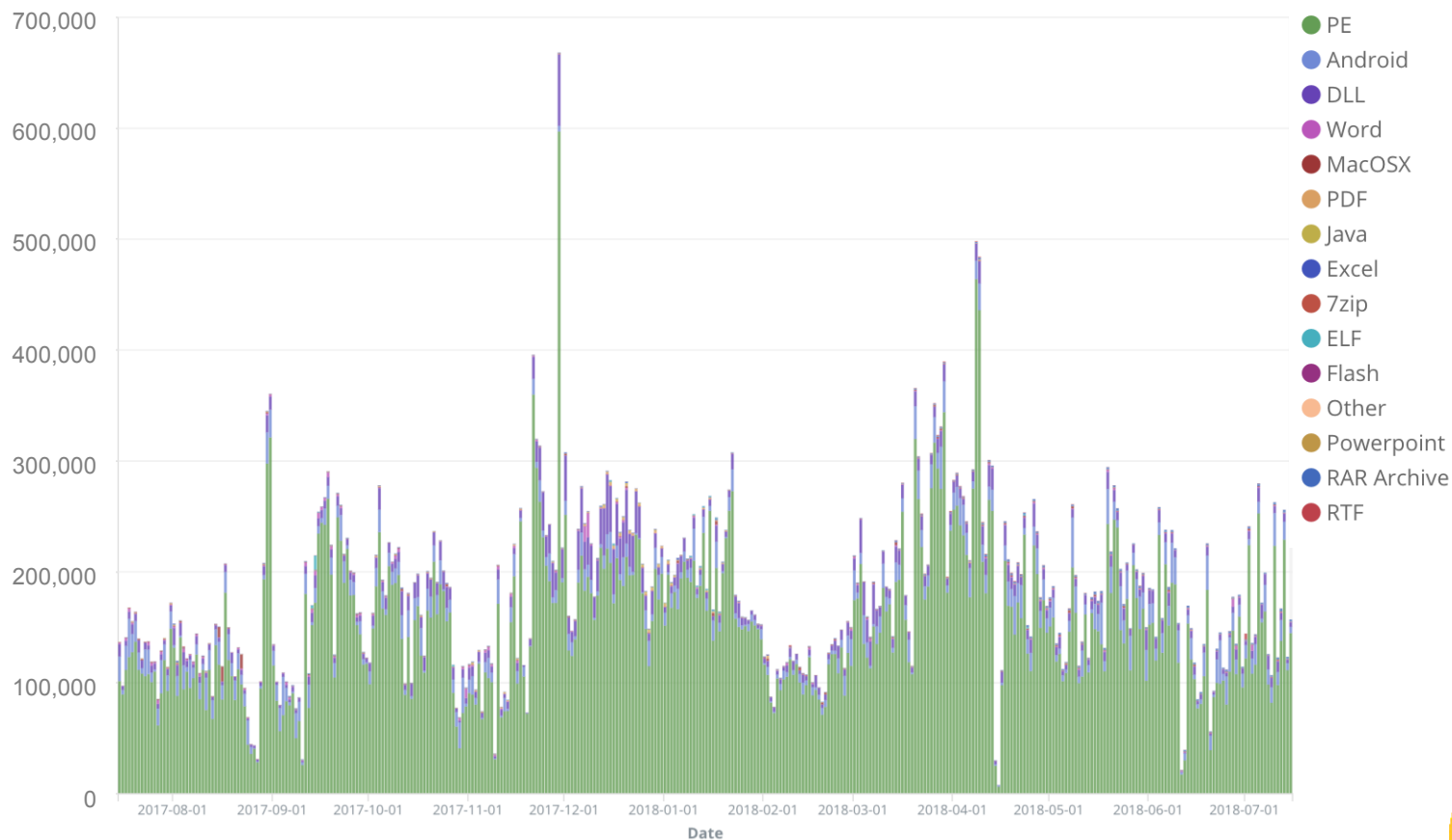
Příchozí vzorky podle typu souboru - všechny



Nový malware – vzorky denně ze všech zdrojů

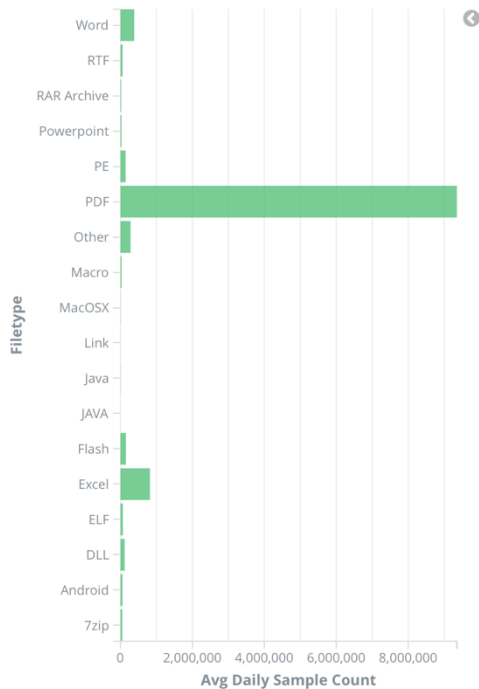


Příchozí malware podle typu souboru

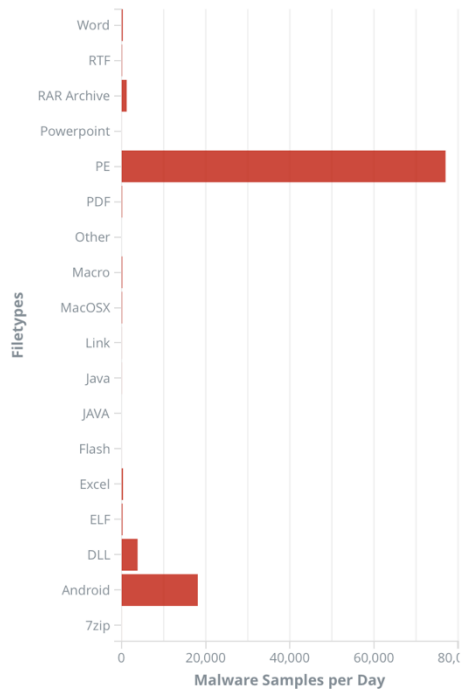


Všechny vzorky vs. malware, podle typů souborů

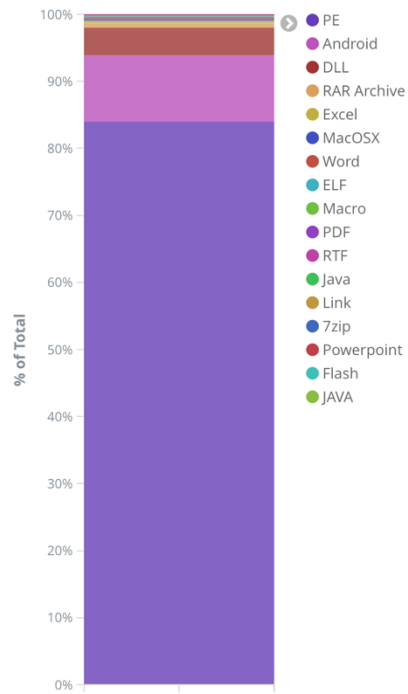
All Samples (Daily)



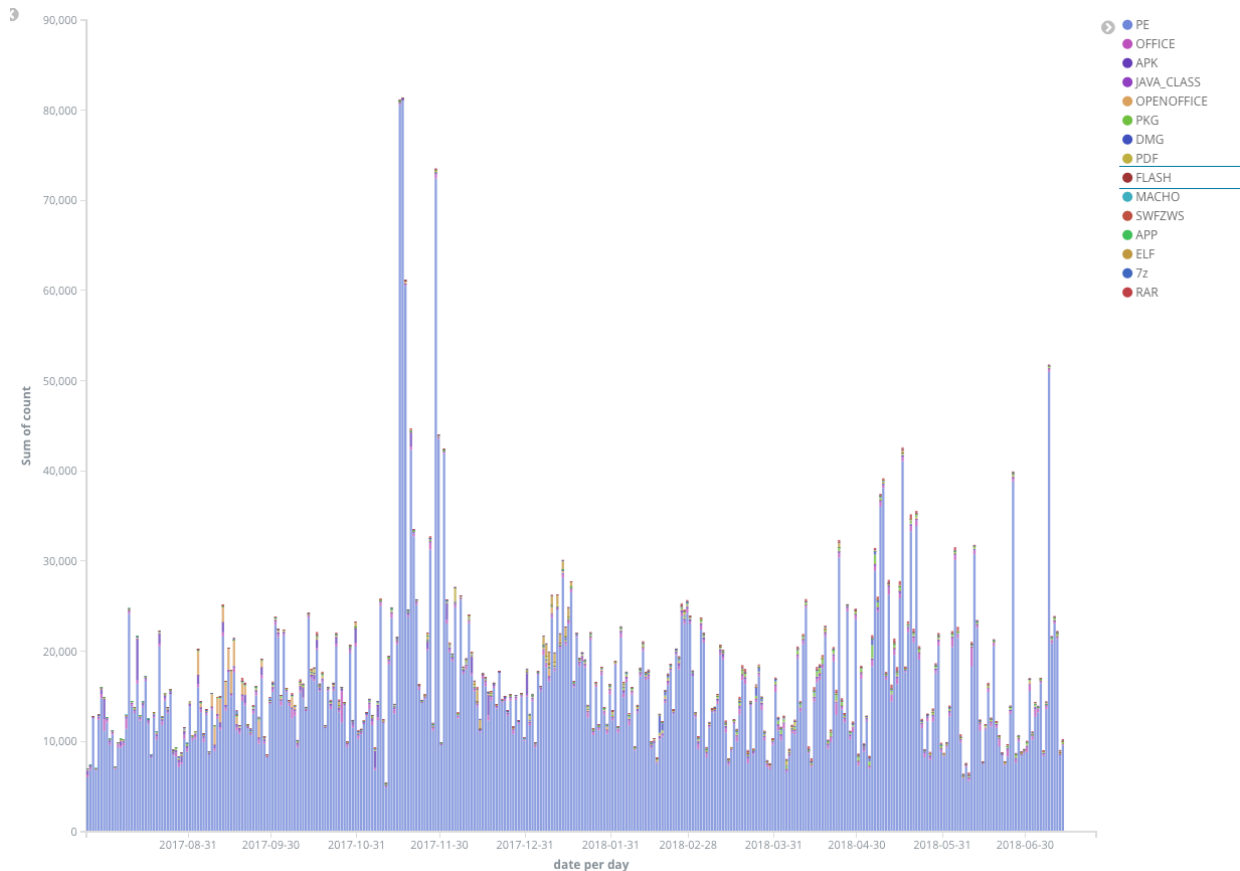
Malware Verdicts (Daily)



% Malware by Filetype

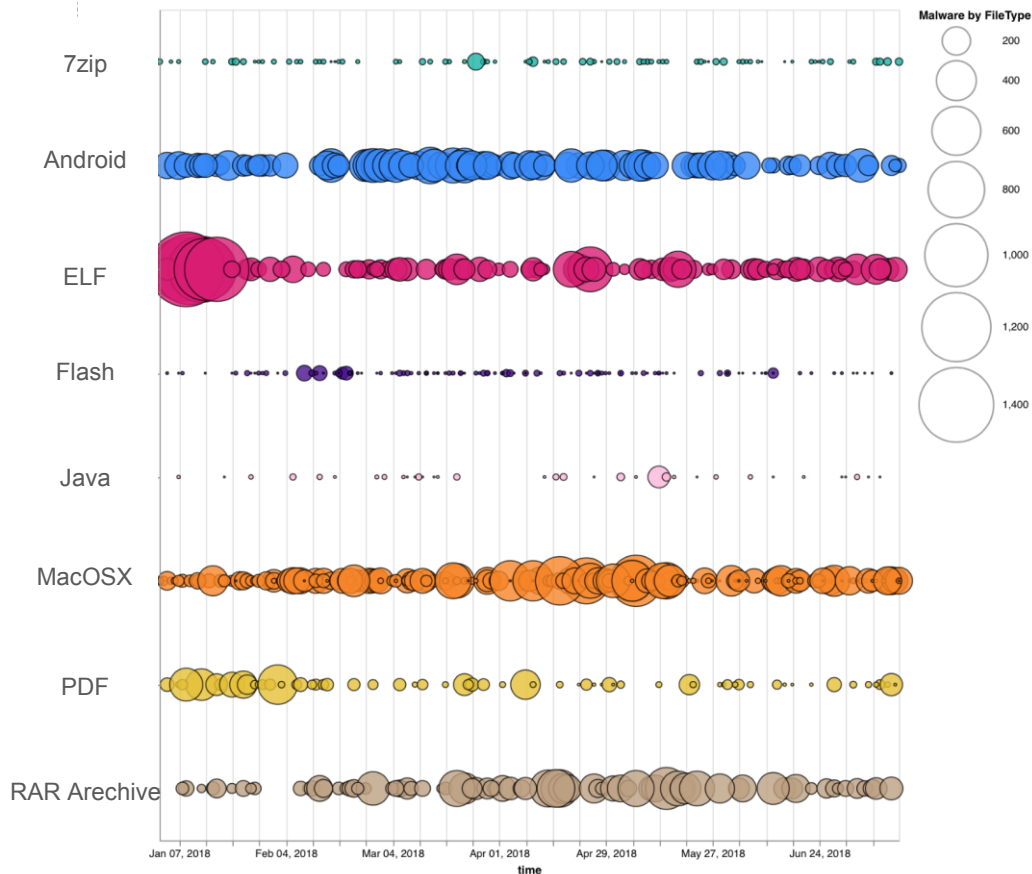


Denní počty AV signatur podle typu souboru



- Většina je PE a spol, PE+DLL jako jeden typ

AV signatury, dle typu souboru, bez PE+DLL



- Na které typy souborů vytváříme nejvíc AV signatur

Stejná signatura pro více příbuzných vzorků malware

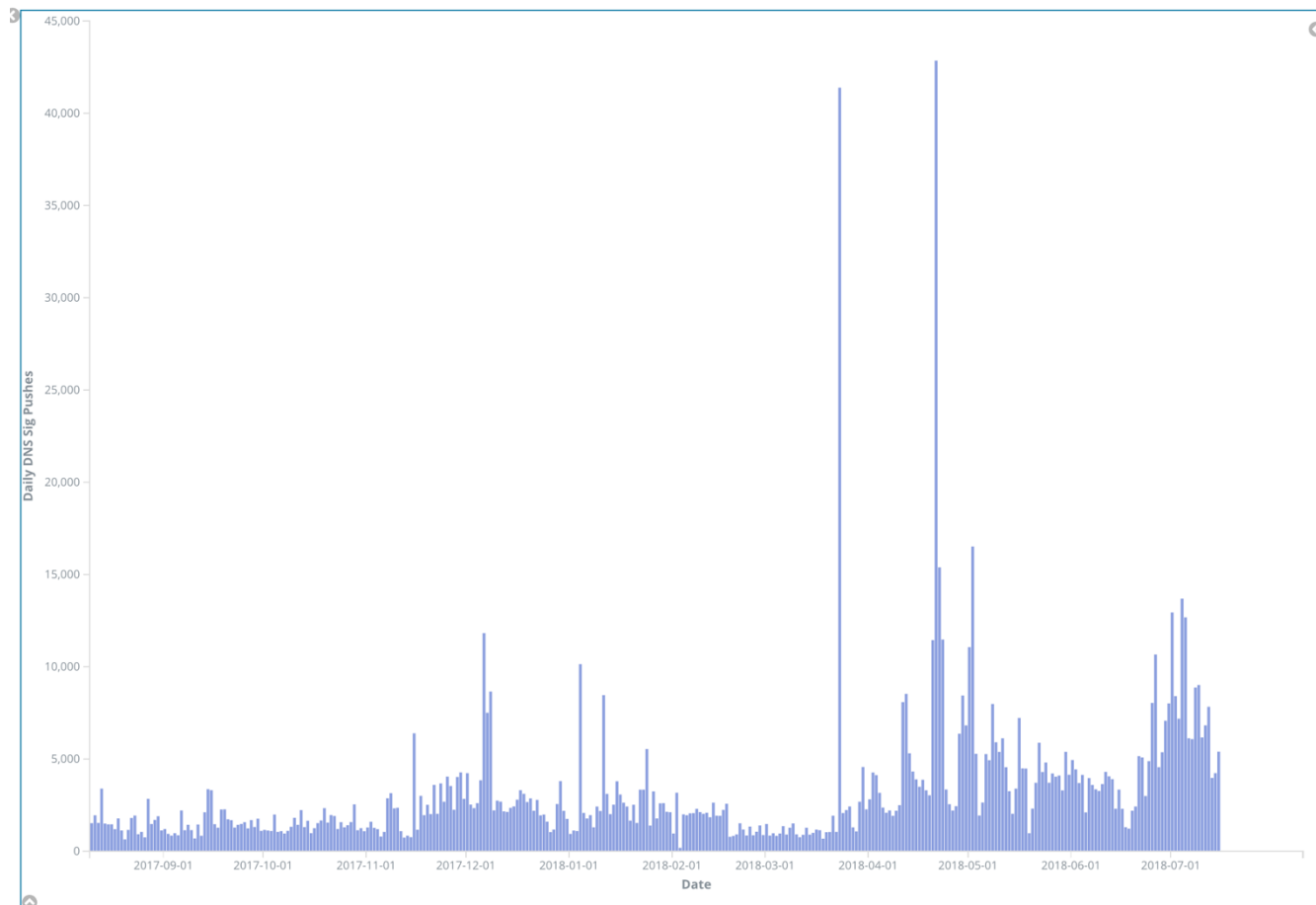
Top 20 aktivních (červenec 2018)

JMÉNO	VZORKŮ
Virus/Win32.parite.etuo	1,248,007
Virus/Win32.madang.ojo	920,382
Virus/Win32.Ipamor.b	896,690
Worm/Win32.fileinfector.fglu	795,526
Trojan/Win32.zbot.xuob	556,844
Virus/Win32.madang.ojx	532,008
TrojanDropper/Win32.lamechi.dmi	526,858
Trojan-Spy/Win32.qukart.xi	338,386
TrojanDropper/Win32.dinwod.adi	315,662
Trojan/Win32.vilsel.ajugl	302,152

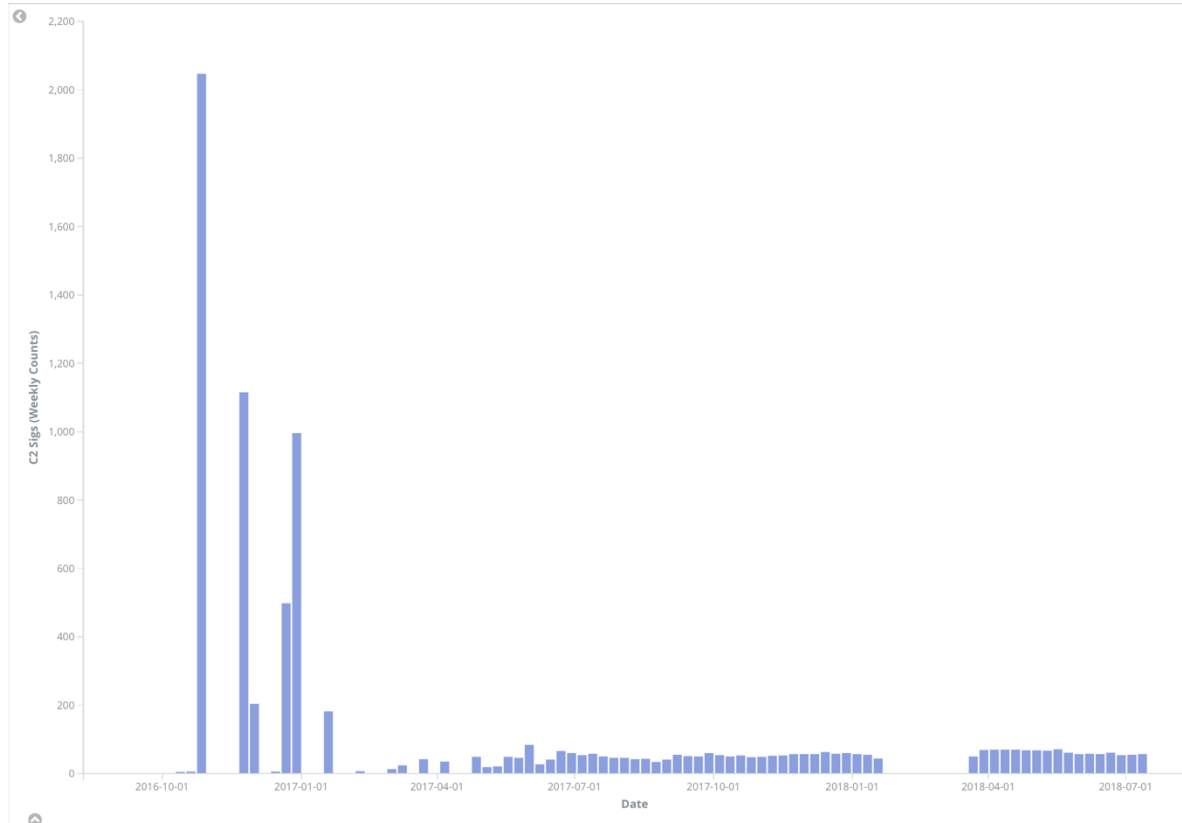
JMÉNO	VZORKŮ
Trojan/Win32.upatre.gpg	296,960
Virus/Win32.parite.xqfd	296,580
Trojan/Win32.upatre.gtx	235,382
Virus/Win32.sillydl.e	213,619
Backdoor/Win32.wabot.alaj	196,390
Virus/Win32.dropper.ut	196,380
Worm/Win32.vb.ckvyk	191,621
Downloader/Win32.fsh.ajr	183,875
Trojan/Win32.Scar.ylz	181,589
Trojan/Win32.cosmu.dggw	153,900

pomocí top 20 AV signatur pokrýváme 8.6 milionu vzorků

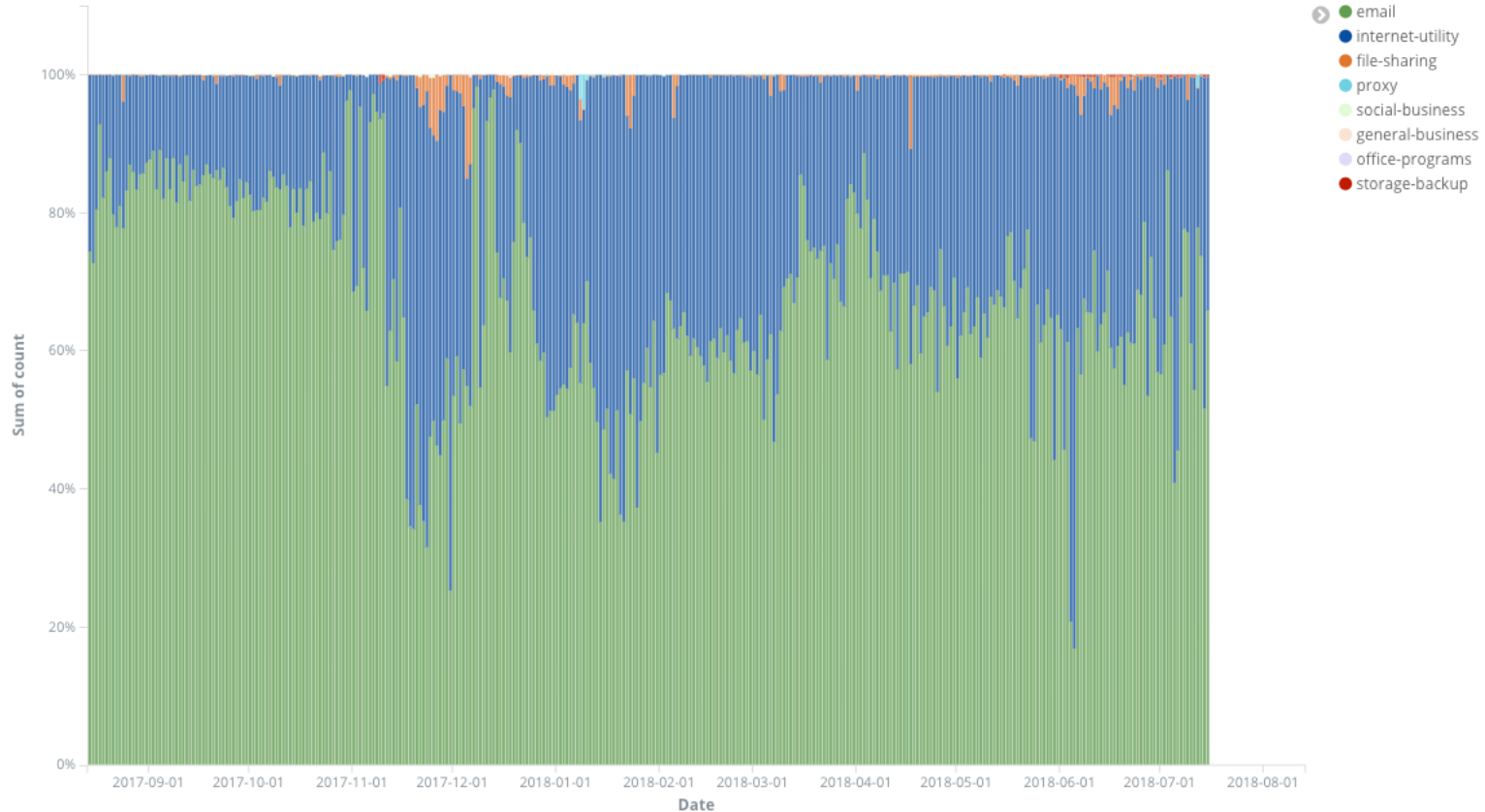
Nové DNS domény aktualizované denně



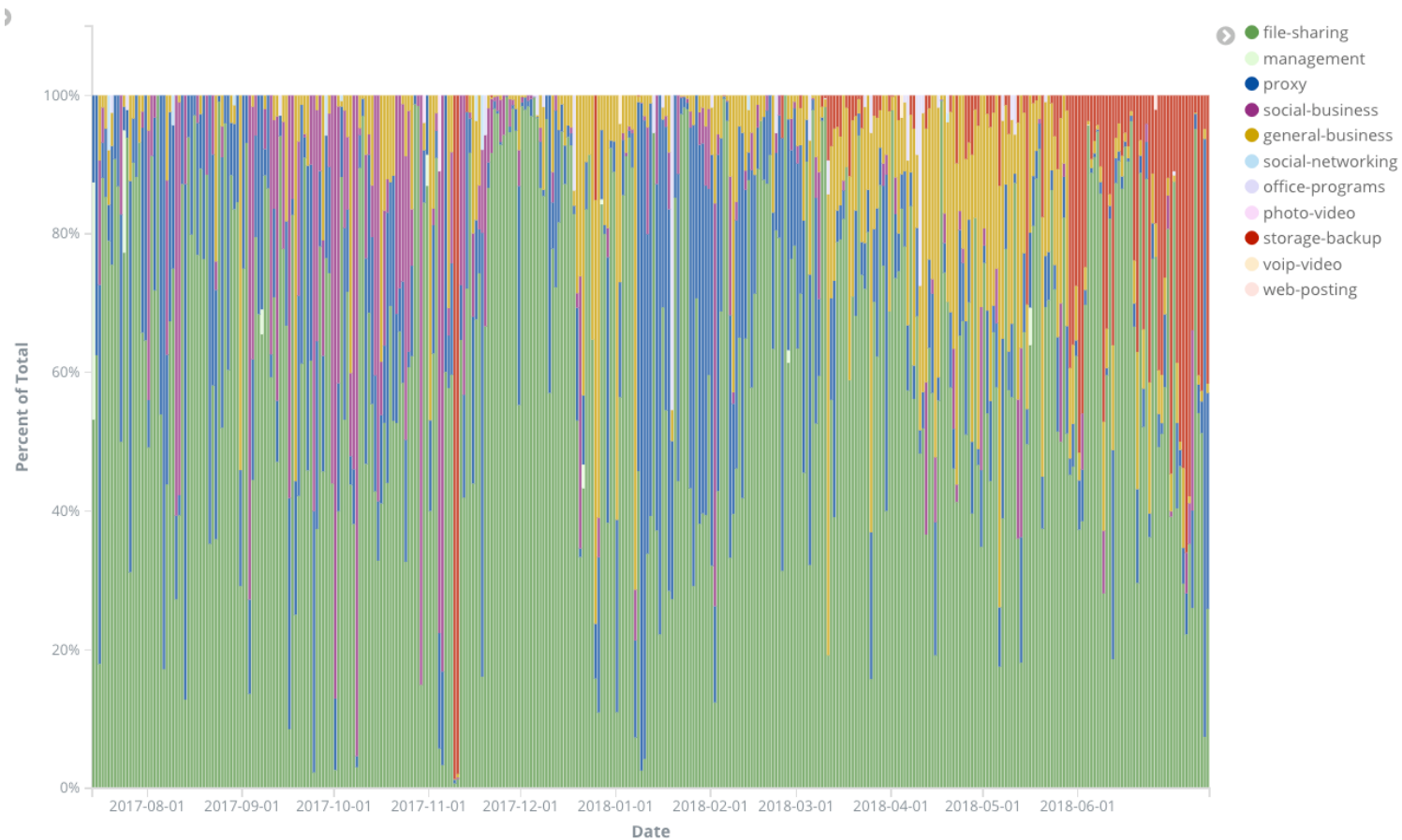
C2 signatury – aktualizace blokuje C2 provoz všude



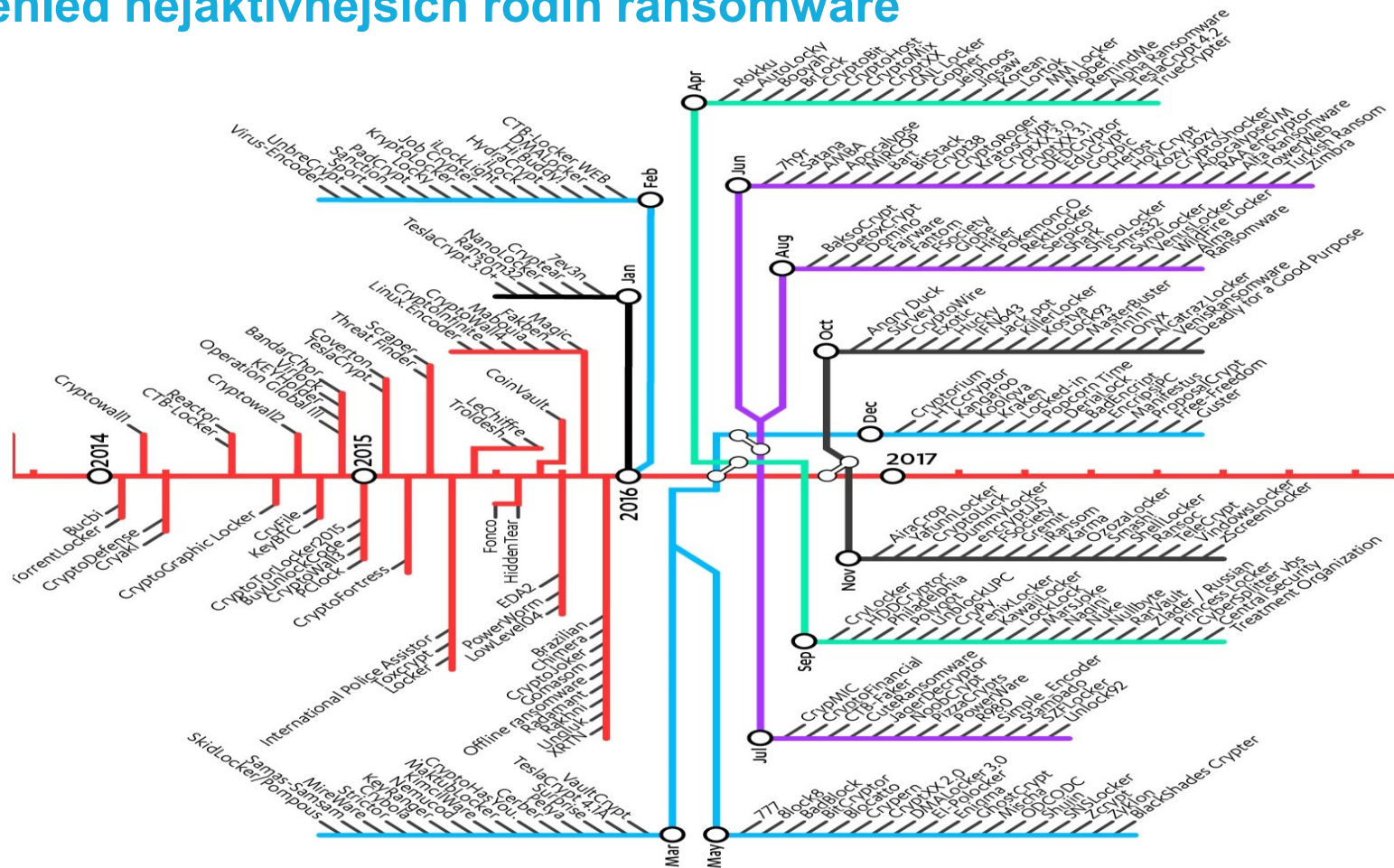
Aplikace podle skupin: všechny kategorie



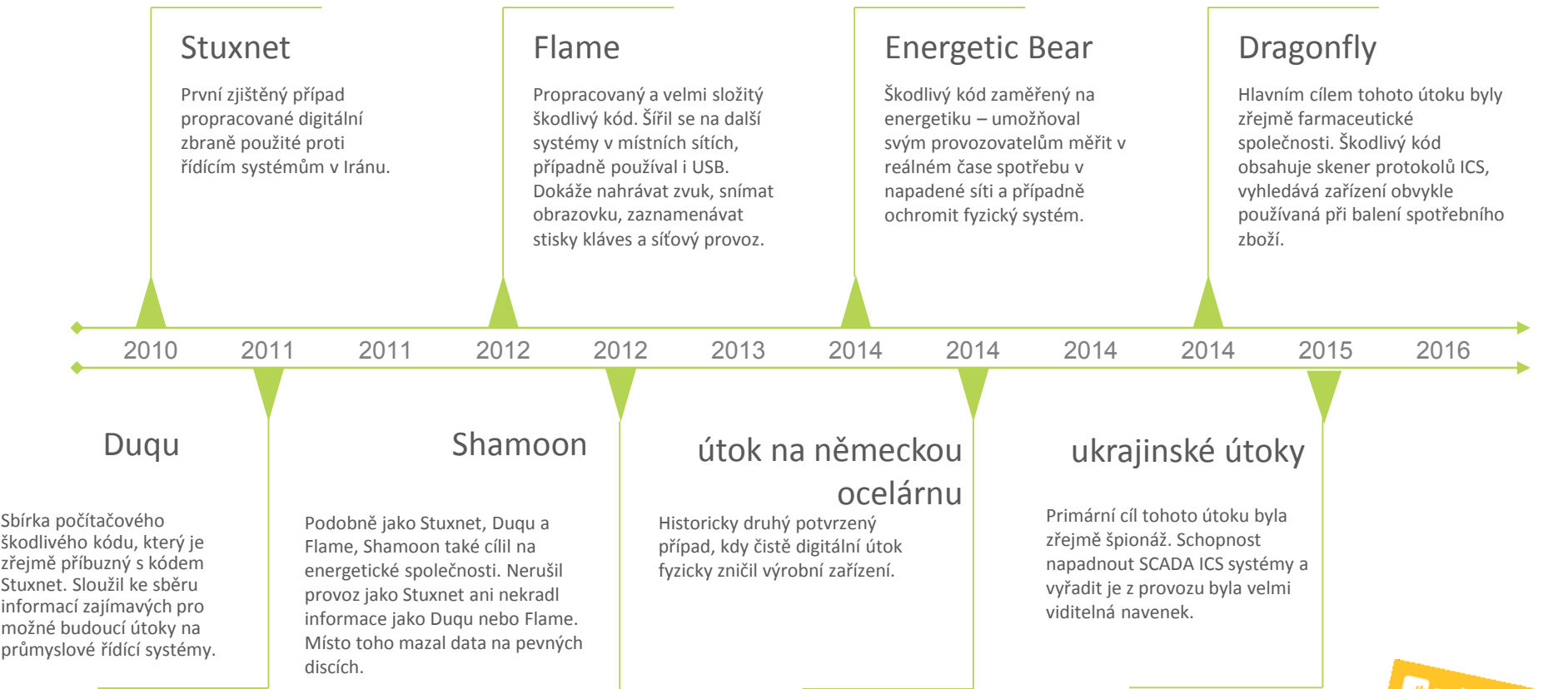
Aplikace podle skupin: bez pošty a webu



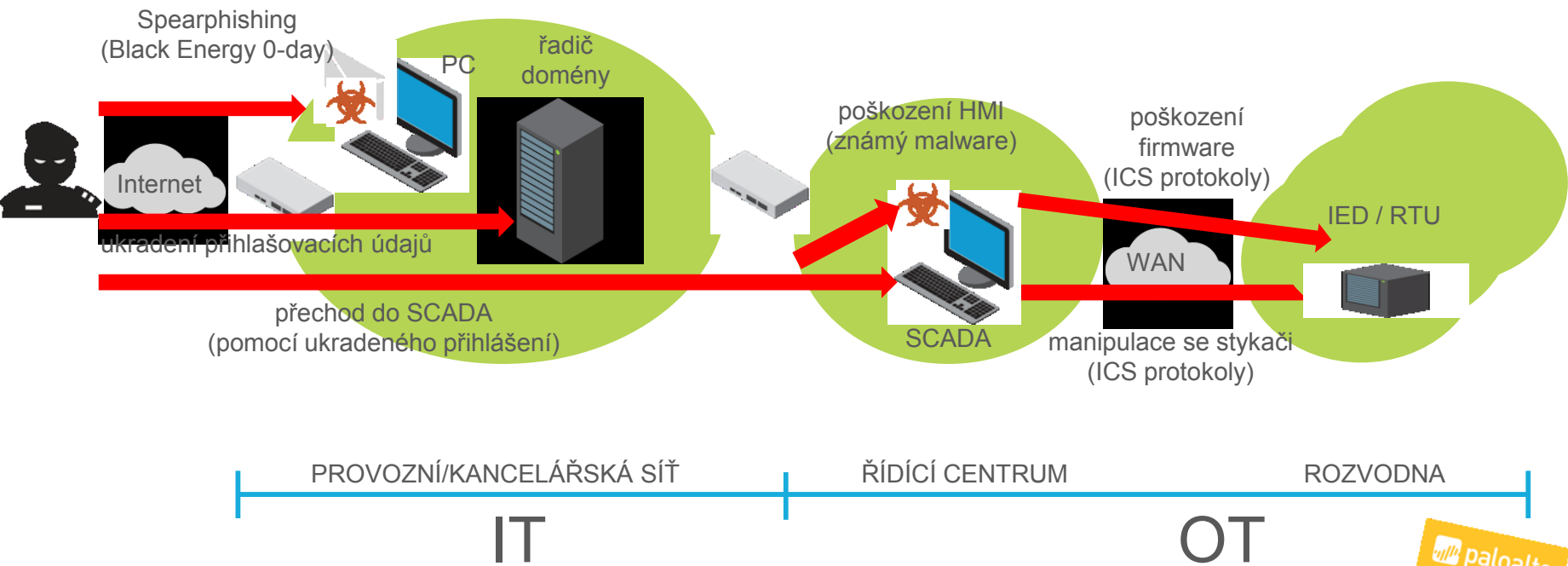
Přehled neaktivnějších rodin ransomware



Nejznámější škodlivý kód zaměřený na kritickou infrastrukturu



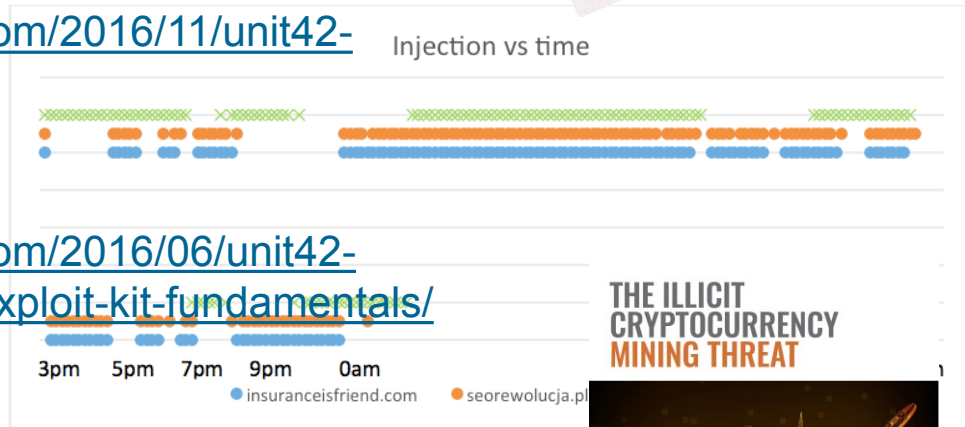
Útoky jsou stále propracovanější - Ukrajina



Zajímavé studie o fungování malware, exploit toolkitů..



- Analýza škodlivého kódu Disttrack/Shamoon 2
 - <http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/>
- Angler EK: vynalézavé ukrývání se
 - <http://researchcenter.paloaltonetworks.com/2016/06/unit42-understanding-angler-exploit-kit-part-1-exploit-kit-fundamentals/>
- CTA: Cryptomining Paper
 - <https://www.cyberthreatalliance.org/resources/wp-content/uploads-2018-09-cta-illicit-cryptomining-key-findings-pdf/>



THE ILLICIT CRYPTOCURRENCY MINING THREAT

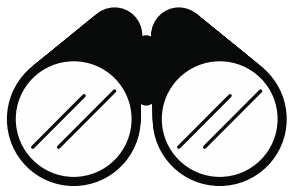


ABSTRACT

Illicit cryptocurrency mining has increased significantly in just a few months. This activity poses both a short- and long-term threat to individuals and enterprises. The threat is not accidental or sporadic, as individuals and organizations should take steps to protect their systems. This report lays out the threat, its potential impact, and the best practices organizations can employ to counter it.



Základní filosofie prevence



**COMPLETE
VISIBILITY**

**ÚPLNÁ
VIDITELNOST**



**REDUCE
ATTACK
SURFACE**

**MENŠÍ PLOCHA
PRO ÚTOK**



**PREVENT
KNOWN
THREATS**

**ZAMEZENÍ VŠEM
ZNÁMÝM HROZBÁM**

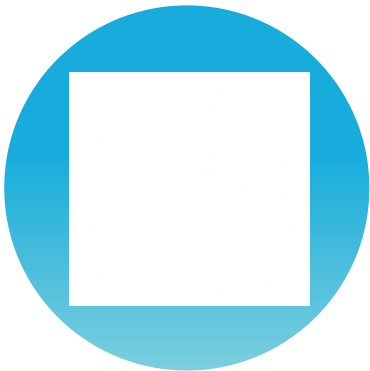


**PREVENT
UNKNOWN
THREATS**

**ZJIŠTĚNÍ A ZASTAVENÍ
NOVÝCH HROZEB**

PLATFORMA SE SOLIDNÍMI ZÁKLADY

NEXT GENERATION FIREWALL



LEADER V BEZPEČNOSTI

nejrychleji rostoucí výrobce

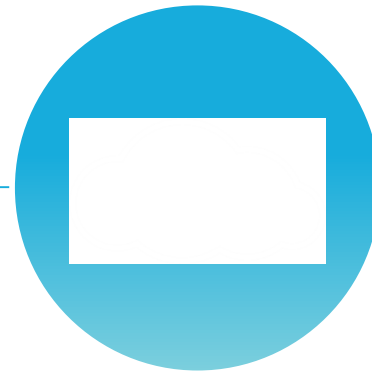
OCHRANA KONCOVÝCH BODŮ



FUNGUJÍCÍ OCHRANA

ransomware a malware
bezsuborové útoky
zneužití zranitelností

ZABEZPEČENÍ V CLOUDU

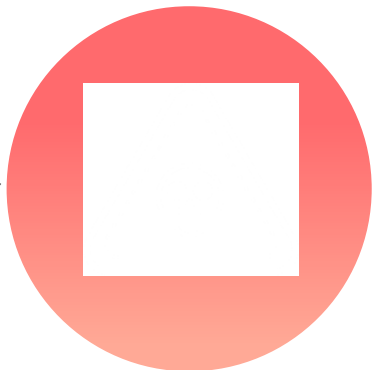


ÚPLNÁ OCHRANA CLOUDU

inline
API
hostitel

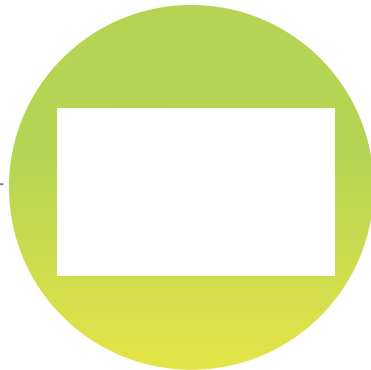
PŘÍSTUP ZERO TRUST SNIŽUJE ŠANCE ÚTOČNÍKŮ

PROBLÉM



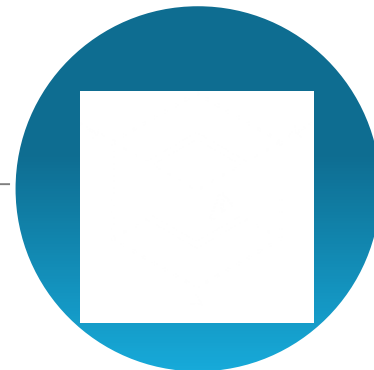
**OTEVŘENÝ PŘÍSTUP
ZVYŠUJE RIZIKA**

OPATŘENÍ



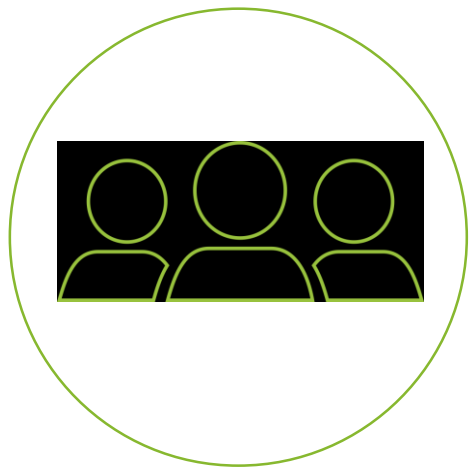
**OMEZENÍ PŘÍSTUPU
K CITLIVÝM
INFORMACÍM**

PŘÍNOSY

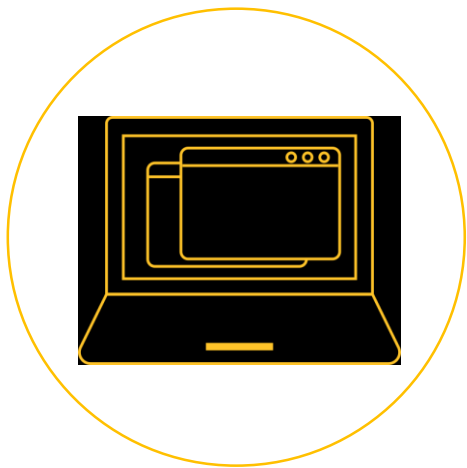


**NIŽŠÍ POČET
INCIDENTŮ**

BEZPEČNÉ A ADRESNÉ POVOLOVÁNÍ APLIKACÍ – POZITIVNÍ PRAVIDLA



UŽIVATEL

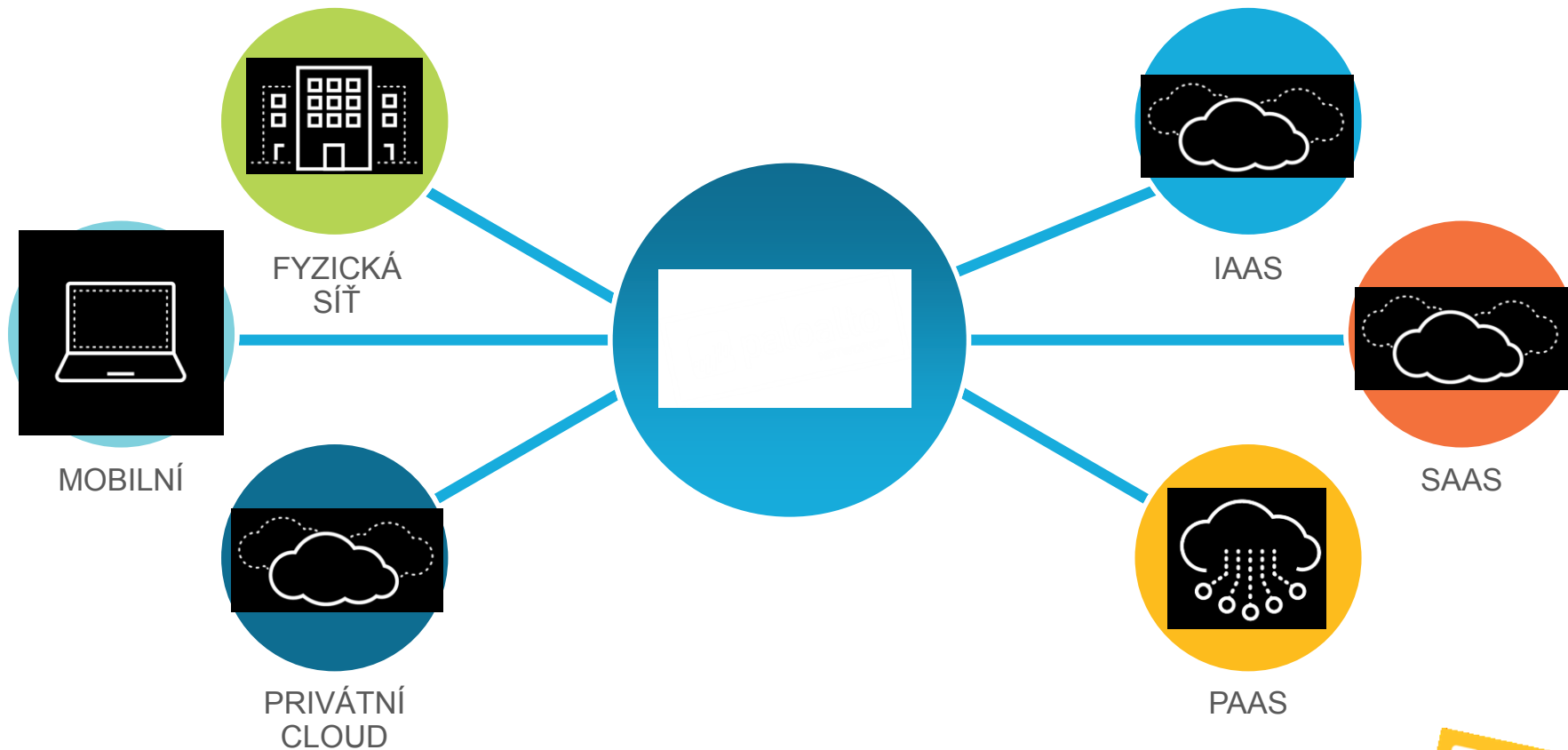


APLIKACE

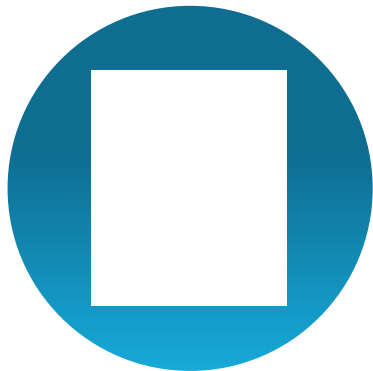


OBSAH

NEUSTÁLÁ PREVENCE NA VŠECH MÍSTECH



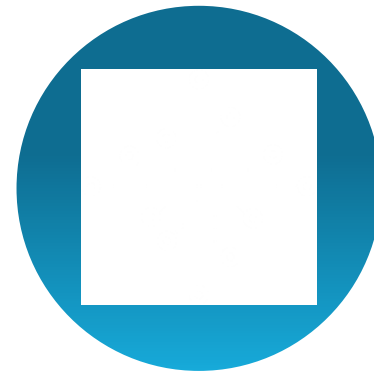
JEN AUTOMATIZACE JE RYCHLEJŠÍ NEŽ ÚTOČNÍCI



OKAMŽITÁ DETEKCE
A ZASTAVENÍ
HROZEB



BEZPEČNOSTNÍ PRAVIDLA
SE DYNAMICKY
PŘIZPŮSOBUJÍ PROSTŘEDÍ



PODNĚTY PŘICHÁZÍ
OD ANALYTIKY A
STROJOVÉHO UČENÍ

PŘÍKLAD OKAMŽITÉHO ZÁSAHU PROTI ÚTOKU

1

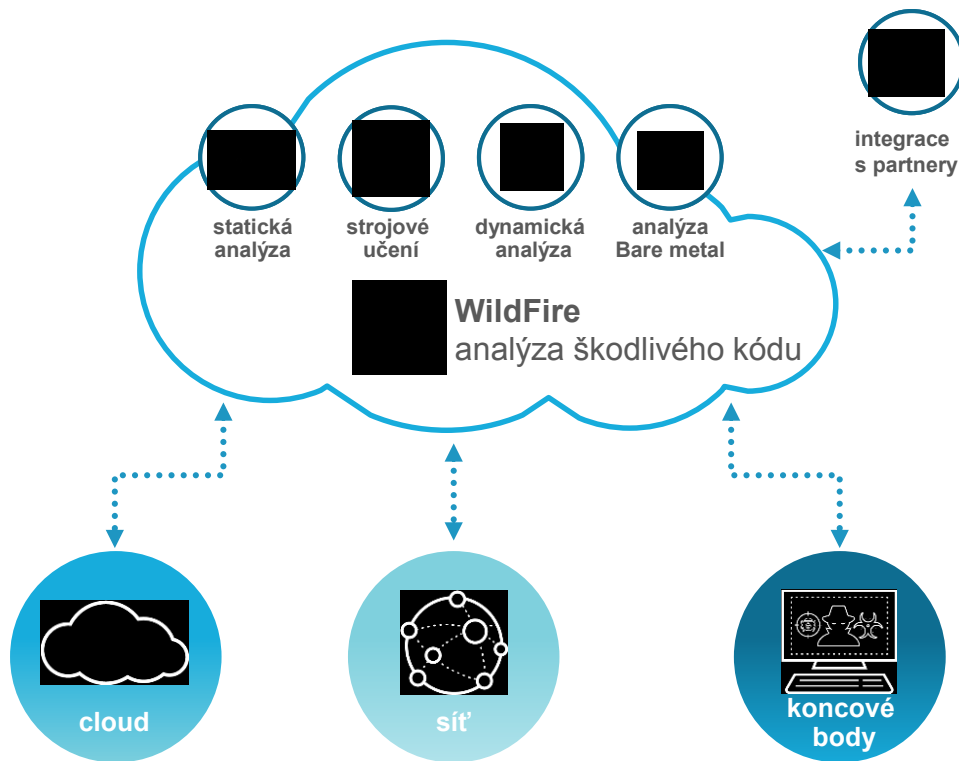
NGFWs, Aperture nebo Traps odešlou neznámý nebo podezřelý soubor nebo odkaz do WildFire

2

WildFire analyzuje neznámé, vytvoří verdikt a sdílí svá zjištění

3

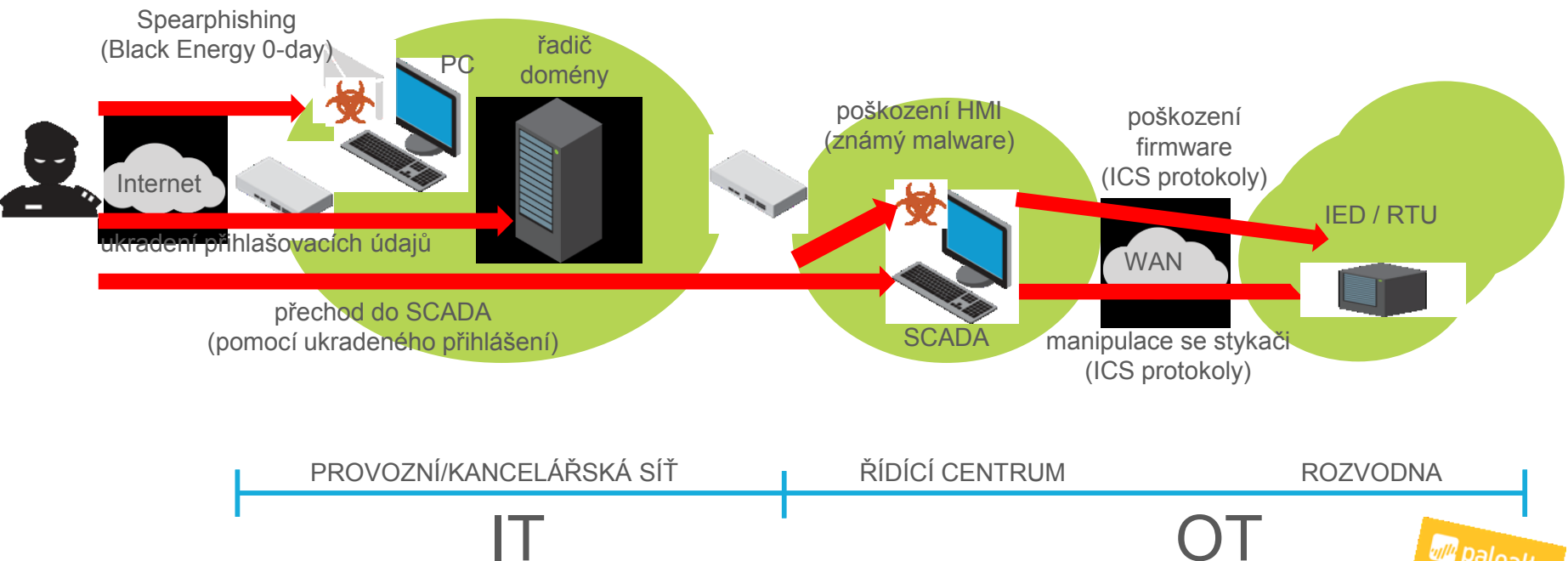
Automatické přenastavení sítě, koncových bodů a cloudu pro zajištění ochrany proti nové hrozbě



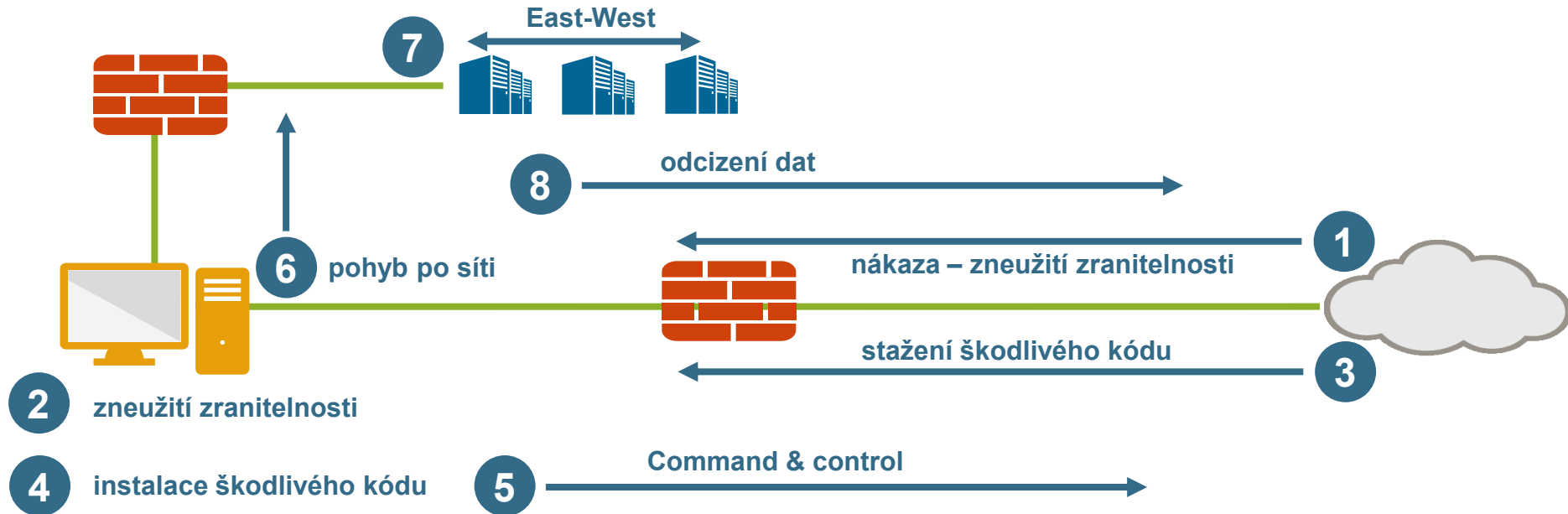
Dobrá prevence vyžaduje kombinaci mnoha specializovaných metod



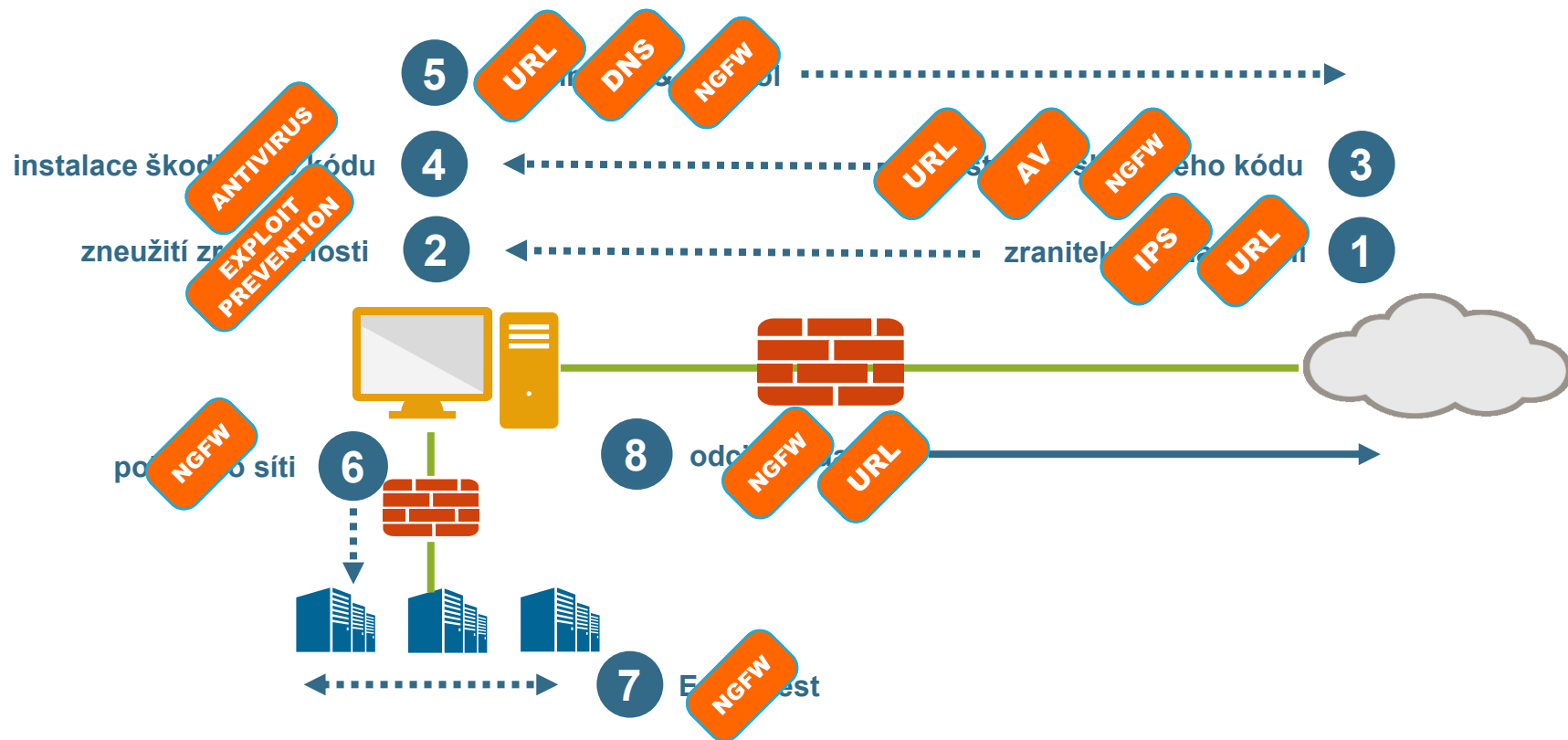
Připomenutí - útoky jsou stále propracovanější



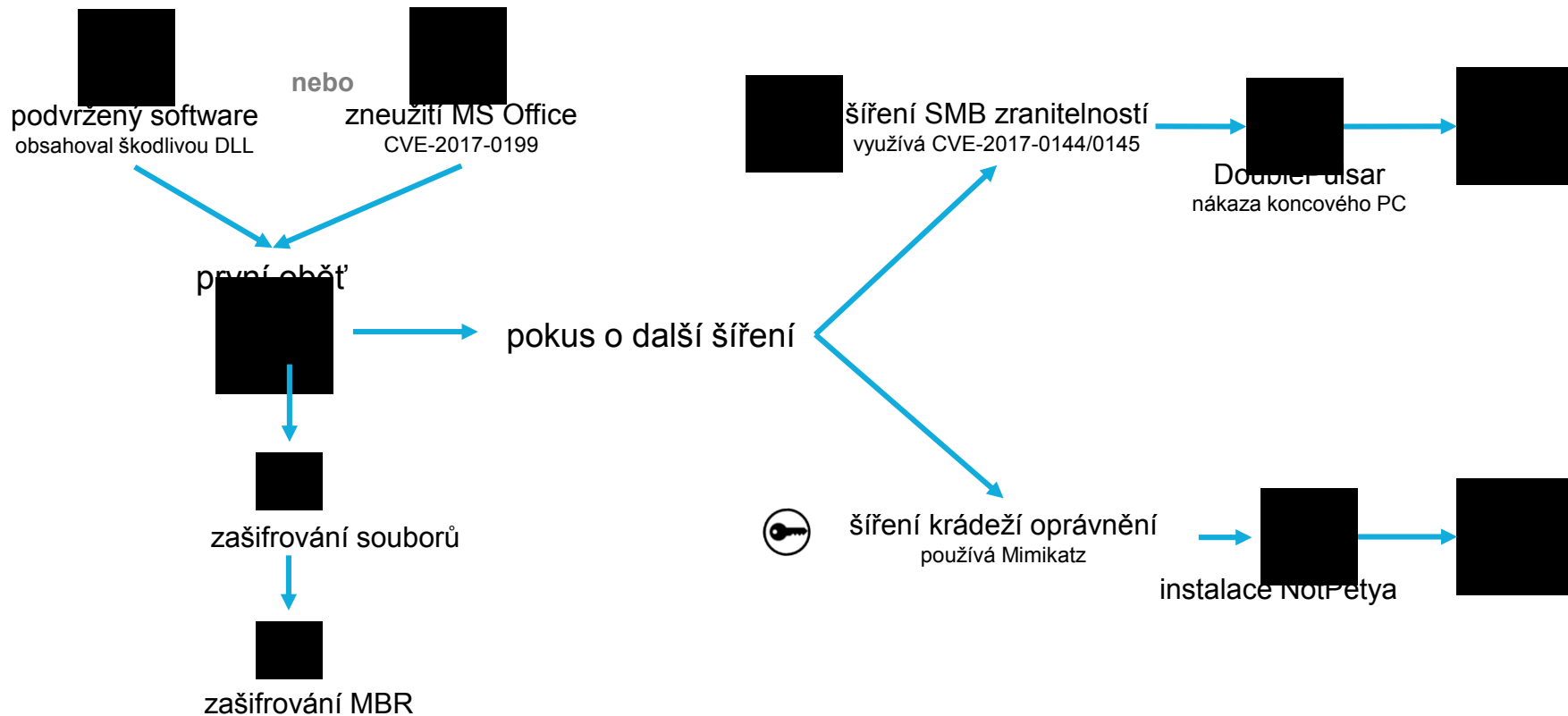
Kde všude lze útočníka zastavit



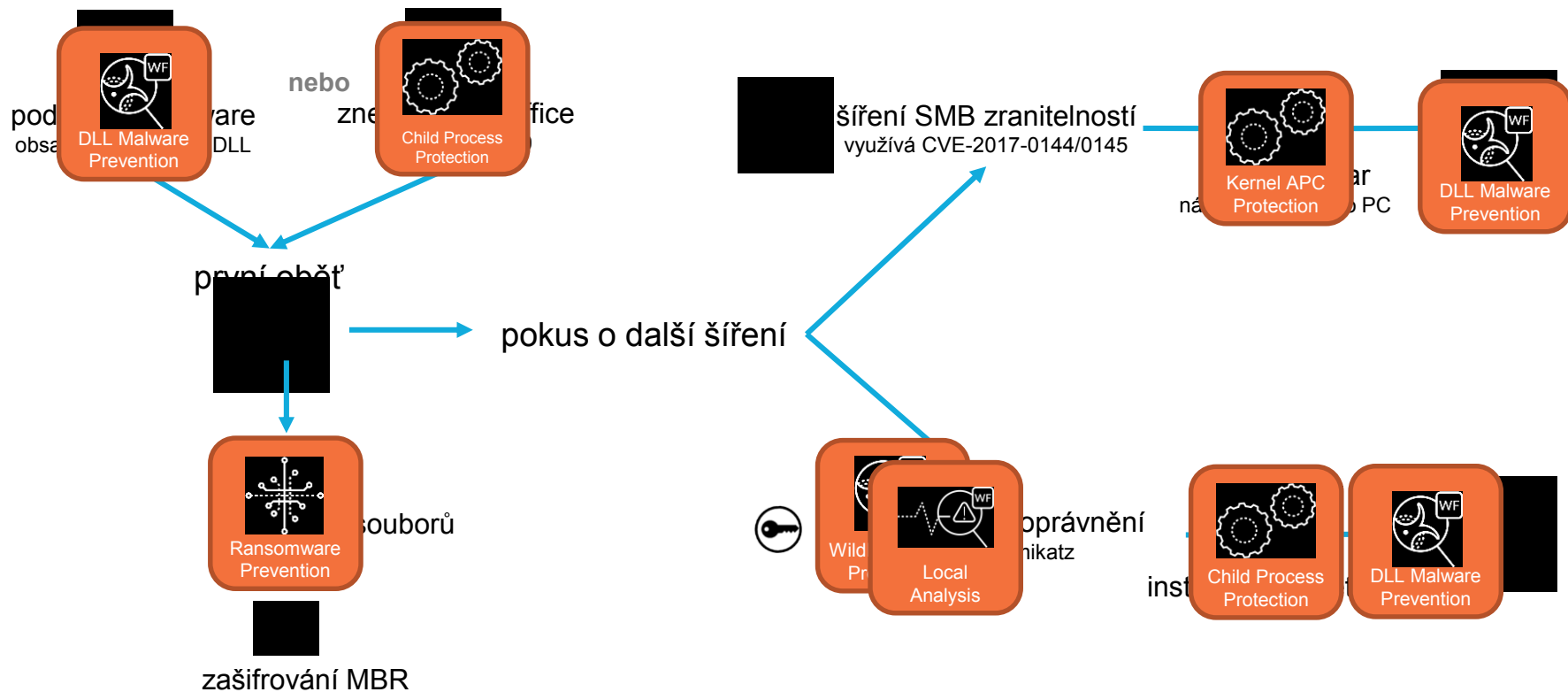
Kde všude lze útočníka zastavit



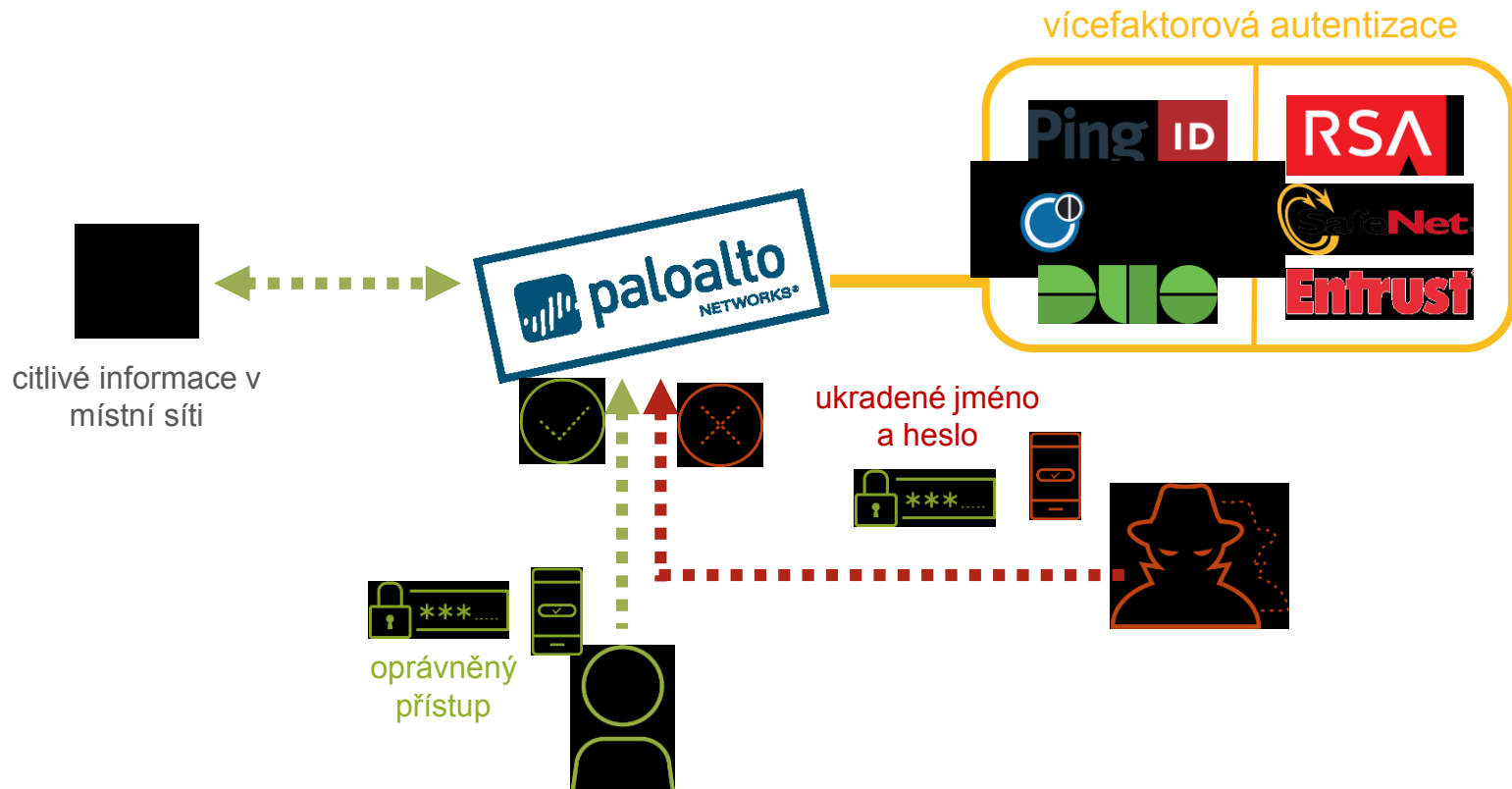
Traps v reálném nasazení – útok NotPetya



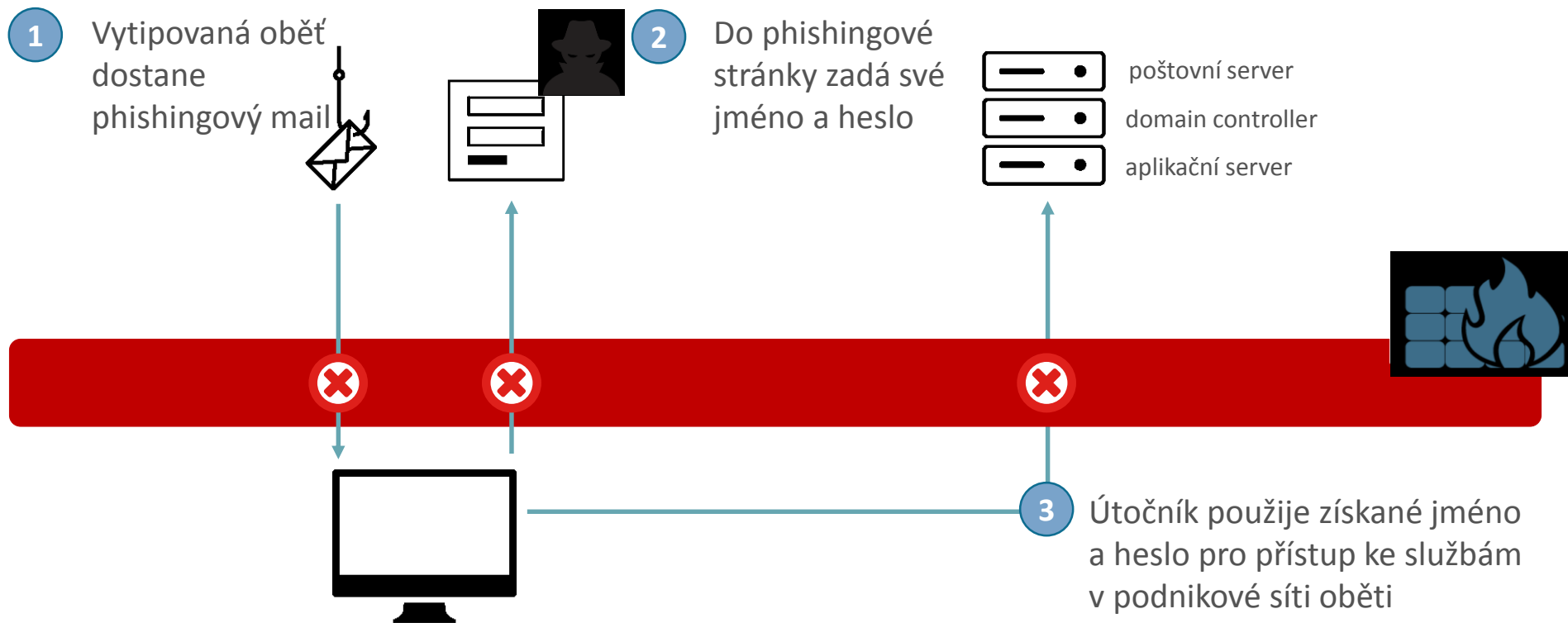
NotPetya – jak to zastavují Traps



Zamezení zneužití přihlašovacích údajů



Útočník při pokusu o zcizení přístupových údajů neuspěl



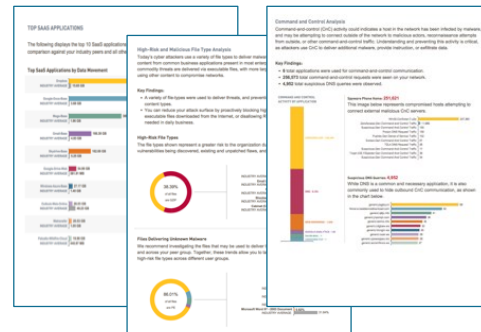
Zmenšení cíle pomocí IP seznamů



- Address Groups - Regions - Applications - Application Groups - Application Filters - Services - Service Groups - Tags - GlobalProtect - HIP Objects - HIP Profiles - External Dynamic Lists - Custom Objects - Data Patterns - Spyware - Vulnerability - URL Category - Security Profiles - Antivirus - Anti-Spyware - Vulnerability Protection - URL Filtering	☐ Name ▲	Location	Description	Source
	▼ Dynamic IP Lists			
	☐ Palo Alto Networks - High risk IP addresses	Predefined	High risk IP addresses, shared IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations, however Palo Alto Networks does not have direct evidence of maliciousness	Palo Alto Networks - High risk IP addresses
	☐ Palo Alto Networks - Known malicious IP addresses	Predefined	Malicious IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, or for launching various attacks	Palo Alto Networks - Known malicious IP addresses
	☐ bbbbbb	Division-marketing (vsys3)		http://test.com
	☐ Malware Domain List	Shared	List of Malicious IPs from Malware Domain List	https://panwdbd.appspot.com...
	▼ Dynamic Domain Lists			
	☐ MineMeld-Domains	Shared		https://10.3.136.199/feeds/af...
	▼ Dynamic URL Lists			
	☐ MineMeld-URLs	Shared		https://10.3.136.199/feeds/af...

Vyzkoušení technologie: Security Lifecycle Review

- Vlastní hodnocení rizik ve vaší organizaci
- Viditelnost na úrovni aplikací, škodlivého kódu, zranitelností ve vaší síti
- Testování po dobu 1-2 týdnů



NAINSTALUJEME ZAŘÍZENÍ
DO VAŠÍ SÍTĚ

PASIVNĚ MONITORUJEME
PROVOZ PO DOBU 1 TÝDNE

PŘIPRAVÍME VÝSTUP S
VÝSLEDKY TESTOVÁNÍ

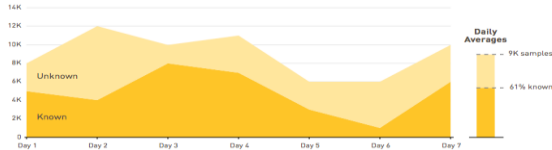
Security Lifecycle Review

- Vyzkoušení (Proof of Concept) Next Generation Security platformy
- Informace o známých a neznámých hrozbách, zranitelnostech, používaných aplikacích

WHAT YOU DON'T KNOW CAN HURT YOU

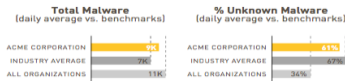
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum irure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugiat nulla facilisis. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad

UNKNOWN VS. KNOWN MALWARE: 7 DAYS



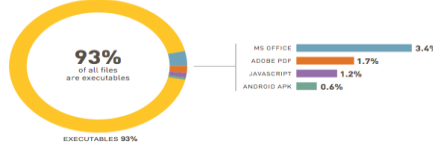
BENCHMARKS

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.



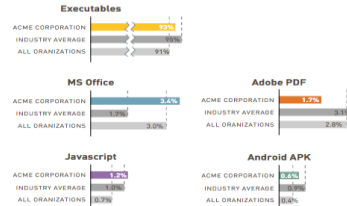
FILE TYPE BREAKDOWN

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum irure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros



BENCHMARKS

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.



WILDFIRE REPORT | PALO ALTO NETWORKS 3

COMMAND & CONTROL ACTIVITY

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam,



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum irure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero

WILDFIRE REPORT | PALO ALTO NETWORKS 6

Ultimate Test Drive

Hands-on LAB s Palo Alto Networks



- Délka workshopu 3 hodiny
- Určené pro technickou komunitu
- Možnost vyzkoušet Next Generation platformu
- Sada praktických cvičení zaměřených na konkrétní bezpečnostní témata: viditelnost aplikací, uživatelskou identitu, sandboxing, SSL dekrypci, ochranu koncových bodů Traps
- Možnost vyhrát zdarma firewall PA-220
- Registrace na **www.nextgenfw.cz**

Jakub Jiříček

Systems Engineer

jjiricek@paloaltonetworks.com

+420-603-552441



Radim Pácl

Regional Sales Manager

rpac1@paloaltonetworks.com

+420-602-362480